2131

Attorney Docket No.: BHT-3092-258 #2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	:	
Wei Kuang TENG	:	Group Art Unit: 2131
Application No.: 10/035,315	:	Examiner: Not Yet Assigned
Filed: January 4, 2002	:	

For: **METHOD FOR DATA SECURITY WITH LOCK IN A HARD DISK AND A SOLID STATE DISK**

CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Pursuant to the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55, Applicant claims the right of priority based upon **Chinese Application No. 01139724.1 filed November 28, 2001.**

A certified copy of Applicant's priority document is submitted herewith.

Respectfully submitted,

By: _____
Bruce H. Troxell
Reg. No. 26,592

TROXELL LAW OFFICE PLLC
5205 Leesburg Pike, Suite 1404
Falls Church, Virginia 22041
Telephone: (703) 575-2711
Telefax: (703) 575-2707

Date: March 13, 2002

#2

证 明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：2001 11 28

申　请　号：01 1 39724.1

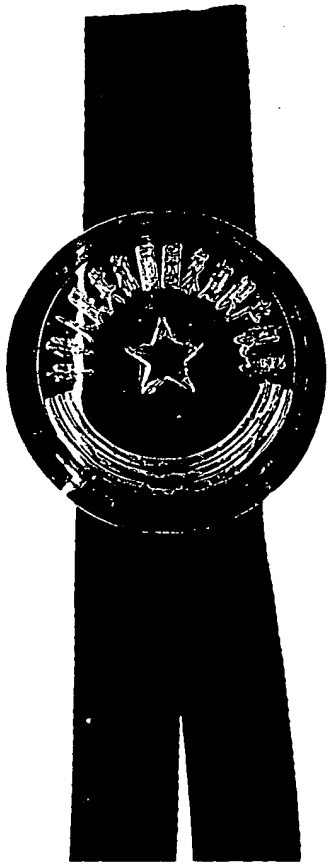
10/035,315- TENG
GAR 2131
BHT-3092-258

申请类别：发明专利

发明创造名称：用于硬盘及固态盘上对资料加密保护资料安全性的方法

申　请　人：劲永国际股份有限公司

发明人或设计人：邓为光



中华人民共和国
国家知识产权局局长 王景川

2002 年 1 月 24 日

权 利 要 求 书

1．一种用于硬盘及固态盘上对资料加密保护资料安全性的方法，其特征在于，该方法包括下列步骤：

对一磁盘机做一磁盘区块分割的程序；

提供复数个暂存器，用以供作为标示该磁盘分割大小的纪录；以及

提供一可对一使用者输入资料与一暂存器资料做数学运算的程序。

2．如权利要求 1 所述的用于硬盘及固态盘上对资料加密保护资料安全性的方法，其特征在于，其中该等暂存器分别为 R_index、P_index 及 LBA_max 暂存器用以作为标示三个分割磁盘区块大小的纪录。

3．如权利要求 1 所述的用于硬盘及固态盘上对资料加密保护资料安全性的方法，其特征在于，其中将分割后的数个磁盘区块指定成一使用者区块、一唯读区块或一保护区块。

4．如权利要求 2 所述的用于硬盘及固态盘上对资料加密保护资料安全性的方法，其特征在于，其中当该等暂存器中 R_index≥1，且暂存器 LBA_max＞P_index＞R_index 时，则磁盘机被分割成为使用者区块、唯读区块、及保护区块等三个区块。

5．如权利要求 2 所述的用于硬盘及固态盘上对资料加密保护资料安全性的方法，其特征在于，其中当该等暂存器 R_index≥1，且暂存器 LBA_max=P_index＞R_index 时，则磁盘机被分割成为使用者区块及唯读区块等二个区块。

6．如权利要求 2 所述的用于硬盘及固态盘上对资料加密保护资料安全性的方法，其特征在于，其中当该等暂存器 R_index≥1，且暂存器 LBA_max＞P_index=R_index 时，则磁盘机被分割成为使用者区块及保护区块等二个区块。

7．如权利要求 2 所述的用于硬盘及固态盘上对资料加密保护资料安全性的方法，其特征在于，其中当该等暂存器 R_index≥1，且暂存器 LBA_max=P_index=R_index 时，则磁盘机只被分割成为使用者区块。

8．如权利要求 1 所述的用于硬盘及固态盘上对资料加密保护资料安

性的方法，其特征在于，其密码运算的方式乃是利用该使用者输入资料与该暂存器资料做一数学运算。

说　　明　　书

用于硬盘及固态盘上对资料加密保护资料安全性的方法

技术领域

本发明是有关一种用于硬盘及固态盘上对资料加密保护资料安全性的方法，尤其是指一种崭新且方便实用的方法以达到对磁盘内存资料安全性的提升。

背景技术

现今对于硬式磁盘（Hard Disk，HD）或固态磁盘（Solid State Disk，SSD）而言，其内部资料的安全性随着资讯家电的普及化而越发重要，不论对系统设计者的内存程序的智慧财产权的权益保障，或是对系统使用者的资料安全维护，保障资料的安全性与否已为一重要的课题。现今的磁盘机于分割后对每一分割的区块皆一视同仁，即每一个分割后的区块皆为可以读、写的区块，并无法区分何者为可读写区块，何者为可唯读区块，及何者为保护区块而不可读写。因此无法满足使用者对于磁盘机资料安全维护的要求。

发明内容

因此本发明的目的是提供一种用于硬盘及固态盘上对资料加密保护资料安全性的方法，该方法可将常用的系统纪录资料存放于“使用者区块”，而将系统主程序或驱动程序存放于“唯读区块”内，以避免程序遭受到不正常或未经允许的变更及更改而破坏系统的运作。而“保护区块”则可存放系统核心程序，其必须透过密码确认始可执行核心程序。因此，本发明可以对磁盘系统作一有效的加密保护功能，使得系统设计者的智慧财产权得以保护，同时对于系统的使用者而言，亦可以达到资料的隐密性与安全性以保护资料，此是为目前已知的各类型磁盘机锁无法企及的功能。

本发明是提供一种用于硬盘及固态盘上对资料加密保护资料安全性的方法，该方法包括下列步骤：对一磁盘机做一磁盘区块分割的程序；提供复数个暂存器，用以供作为标示该磁盘分割大小的纪录；以及提供一可对一“使用者输入资料”与一“暂存器资料”做数学运算的程序。

为了达到上述的目的，本发明一种用于硬盘及固态盘上对资料加密保护资料安全性的方法，该方法包括下列步骤：对一磁盘机做一磁盘区块分割的程序；提供复数个暂存器，用以供作为标示该磁盘分割大小的纪录；以及提供一可对一使用者输入资料与一暂存器资料做数学运算的程序。

其中该等暂存器分别为 R_index、P_index 及 LBA_max 暂存器用以作为标示三个分割磁盘区块大小的纪录。

其中将分割后的数个磁盘区块指定成一使用者区块、一唯读区块或一保护区块。

其中当该等暂存器中 R_index≥1，且暂存器 LBA_max>P_index>R_index 时，则磁盘机被分割成为使用者区块、唯读区块、及保护区块等三个区块。

其中当该等暂存器 R_index≥1，且暂存器 LBA_max=P_index>R_index 时，则磁盘机被分割成为使用者区块及唯读区块等二个区块。

其中当该等暂存器 R_index≥1，且暂存器 LBA_max>P_index=R_index 时，则磁盘机被分割成为使用者区块及保护区块等二个区块。

其中当该等暂存器 R_index≥1，且暂存器 LBA_max=P_index=R_index 时，则磁盘机只被分割成为使用者区块。

其密码运算的方式乃是利用该使用者输入资料与该暂存器资料做一数学运算。以达到资料的隐密性与安全性以保护资料的目的。

附图说明

为使审查员能进一步了解本发明的结构、特征及其目的，以下结合附图及较佳具体实施例的详细说明如后，其中：

图 1 是本发明一较佳实施例的动作流程图；

图 2 是本发明一较佳实施例的于加密模式中的磁盘指令对各区块动作图；

图 3 是本发明一较佳实施例的磁盘分割示意图；

图 4 是本发明一较佳实施例的各种暂存器结构图；

图 5 是本发明一较佳实施例的供应者码及供应者锁的设定流程图；

图 6 是本发明一较佳实施例的固件对密码运算方式的示意图；以及

图 7 是本发明一较佳实施例的唯读区块及保护区块的功能解除流程图。

具体实施方式

请参照图 1，其绘示依照本发明的较佳实施例的动作流程图。如图所示，本发明的一种用于硬盘及固态盘上对资料加密保护资料安全性的方法，首先以磁盘分割（Disk Partition）的方式将磁盘机 1 实体切分为数个区块，例如，将一个磁盘机 1 实体切分为二个或三个逻辑磁盘，并将所分割的逻辑磁盘给于区块定义并加以读或写的限制，使其达到特定的功能。

因此，本发明首先定义出三种区块名称（图 3 中），即“唯读区块”（ROM zone）11，“保护区块”（Protect zone）12 及“使用者区块”（User zone）13。因此一个磁盘机 1 实体可被四种不同排列组合的切割方式进行磁盘分割：

（1）使用者区块 13、唯读区块 11 及保护区块 12；

（2）使用者区块 13 及唯读区块 11；

（3）使用者区块 13 及保护区块 12；

（4）使用者区块 13；

等四种切割方式。

其中的“使用者区块”13，如同一般磁盘机可执行所有的磁盘指令（ATA command），而“唯读区块”11 则只能读取资料而不能对资料进行删除（Erase）或写入（Write），“保护区块”12 则指在此区域内部执行任何对磁盘区段（Sector）动作的指令（请另参照图 2，“于加密模式中的磁盘指令对各区块动作图”的说明），故在此保护区块 12 中无法对

资料进行读取、写入的动作而达到保护的功能。

每个区块的大小可由使用者经适当的工具程序（Utility）自行决定，例如 DOS 的 FDISK 或 Disk Edit 等磁盘切割程序，以提供较方便的方式进行磁盘机 1 的区块分割。而唯读区块 11 及保护区块 12 在未经致能（Enable）前，其功能与使用者区块 13 一样，可执行所有的磁盘指令。

当磁盘机 1 实体被分割后，为了纪录各区块的大小及其在磁盘机 1 中的实体位置，因此建立了“R_index”111、“P_index”121 及“LBA_max”131 等三个暂存器以纪录各区块在磁盘机 1 中的实体位置。

请参照图 3，其绘示依照本发明的较佳实施例的磁盘分割示意图。如图所示此三个暂存器（Register）“R_index”111、“P_index”121 及“LBA_max”131 的意义，而运用此三个参数，即可作为磁盘分割的判断。其判断的法则如下：

（1）当暂存器 R_index≥1，且暂存器 LBA_max＞P_index＞R_index 时，则磁盘机 1 被分割成为使用者区块 13、唯读区块 11、及保护区块 12 等三个区块。

（2）当暂存器 R_index≥1，且暂存器 LBA_max=P_index＞R_index 时，则磁盘机 1 被分割成为使用者区块 13 及唯读区块 11 等二个区块。

（3）当暂存器 R_index≥1，且暂存器 LBA_max＞P_index=R_index 时，则磁盘机 1 被分割成为使用者区块 13 及保护区块 12 等二个区块。

（4）当暂存器 R_index≥1，且暂存器 LBA_max=P_index=R_index 时，则磁盘机 1 只被分割成为使用者区块 13。

其中 R_index 111、P_index 121 及 LBA_max 131 等三个暂存器的设定是透过工具程序的方式来设定，例如工具程序（Utility）A，可自动由磁盘机 1 的主启动纪录（Master Boot Record，MBR）中找各区块的长度，经计算后设定 R_index 111、P_index 121 及 LBA_max 131 等三个暂存器的值。

当唯读区块 11 及保护区块 12 建立后，在未设定密码之前，以上两区块与使用者区块 13 一般，可执行所有的磁盘指令（ATA Command），此时 R_password 30 及 P_password 31 为内定值（Default Value），其值为“0xFFFFFF”一旦 R_password 30 或 P_password 31 被设定后，亦即

R_password 30 或 P_password 31 不为“0xFFFFFF”时，唯读区块 11 或保护区块 12 的区块相关功能经由磁盘控制固件（Firmware）致能后随即开始启动。

当电源启动（Power On）后或任何方式的系统重置（System Reset）时，而磁盘控制固件侦测到 R_password 30 或 P_password 31 不为内定值时，则唯读区块 11 或保护区块 12 的资料保护功能即启动。但如果唯读区块 11 不存在，则 P_password 31 功能亦被禁止。

请再参照图 4，其绘示依照本发明的较佳实施例的各种暂存器结构图。如图所示，其表示了与密码设计相关的暂存器结构，其中 R_password 30 及 P_password 31 可由外部程序来设定。

系统设计者可拥有一控制码，于此处称为一“供应者码”（Vendor Code）20，其是一独立的控制码，而“供应者锁”（Vendor Key）21 则由系统设定者设定，类似批号的处理，两者均由一独立的外部应用程序，例如工具程序 B，输入。而“锁号”（Key Number）40、41 则由系统使用者经由上述工具程序 A 来设定。“锁号”40、41 的 8 位元中仅有 7 位元有效，其定义为在 128 组密码中的第 n 组密码是有效的。因为任一组密码的大小均为 4 个位元组（Bytes），故每次查核密码时有 512 个位元组的密码需进行辨识。“供应者码”20 及“供应者锁”21 的设定流程，请参照图 5，“供应者码”及“供应者锁”的设定流程图。

当 R_password 30 及 P_password 31 被设定后，则表示唯读区块 11 或保护区块 12 功能启动或被锁住（Lock）。如要解除（Unlock）唯读区块 11 或保护区块 12 功能，则必须透过特殊的磁盘指令的方式进行查核及开锁机制。如密码查核失败时，则唯读区块 11 或保护区块 12 的功能立即启动。

如表一所示，即为本发明的密码侦测的磁盘指令定义：其包括有本发明特别定义的 ATA 指令码（FEh），输入规则描述，错误回应描述及指令说明。

表一、密码侦检 ATA 指令

指令码-FEh

定址(Address)	ATA	定义码值(Default)
0×1f7	Command	0×FE
0×1f6	Drv/Head	------
0×1f5	CylMSB	------
0×1f4	CylLSB	------
0×1f3	SecNum	-------
0×1f2	SecNum	0×FE
0×1f1	Feature Cmd	0×AA/0×BB

0×AA：表示为 R_password 30 侦检

0×BB：表示为 P_password 31 侦检

错误回应输出-若无支援此指令，则元件将回应至错误暂存器的 ABRT，资料友唯读区块 11 或保护区块 12 内。

状态暂存器				错误暂存器			
RDY	DWF	CORR	ERR	UNC	IDNF	ABRT	AMNF
×	×		×			×	

指令描述-此指令将要求从系统端（Host）传送一个磁盘区段的资料，而藉由此资料来控制指令的功能。

请参照图 6，其绘示本发明一较佳实施例的固件对密码运算方式的示意图。当固件程序从 128 组密码中取得由锁号 40、41 所指定的有效密码 22 后，则进行如图 6 所示的计算流程，如果计算结果与 R_password 30 或 P_password 31 相同，则将唯读区块 11 或保护区块 12 的功能解除释放，亦即将唯读区块 11 或保护区块 12 的唯读或保护功能禁能，使其如同使用者区块 13 一样可自由读写资料。

请参照图 7，其绘示本发明一较佳实施例的唯读区块及保护区块的功能解除流程图。

所以，经由本发明的实施，可将常用的系统纪录资料存放于“使用

区块”13，而将系统主程序或驱动程序存放于“唯读区块”11 内，以避免程序遭受到不正常或未经允许的变更及更改而破坏系统的运作。而“保护区块”12 则可存放系统核心程序，其必须透过密码确认始可执行核心程序。因此其可以对磁盘系统座一有效的加密保护功能，使得系统设计者的智慧财产得以保护，同时对于系统的使用者而言，亦可以达到资料的隐密性与安全性以保护资料，此是为目前习知的各类型磁盘机锁无法企及的功能者。

虽然本发明已以较佳实施例揭露如上，然其并非用以限定本发明，任何熟习此技艺者，在不脱离本发明的精神和范围内，当可作少许的更动与润饰，因此本发明的保护范围当视后附的申请专利范围所界定者为准。

说 明 书 附 图

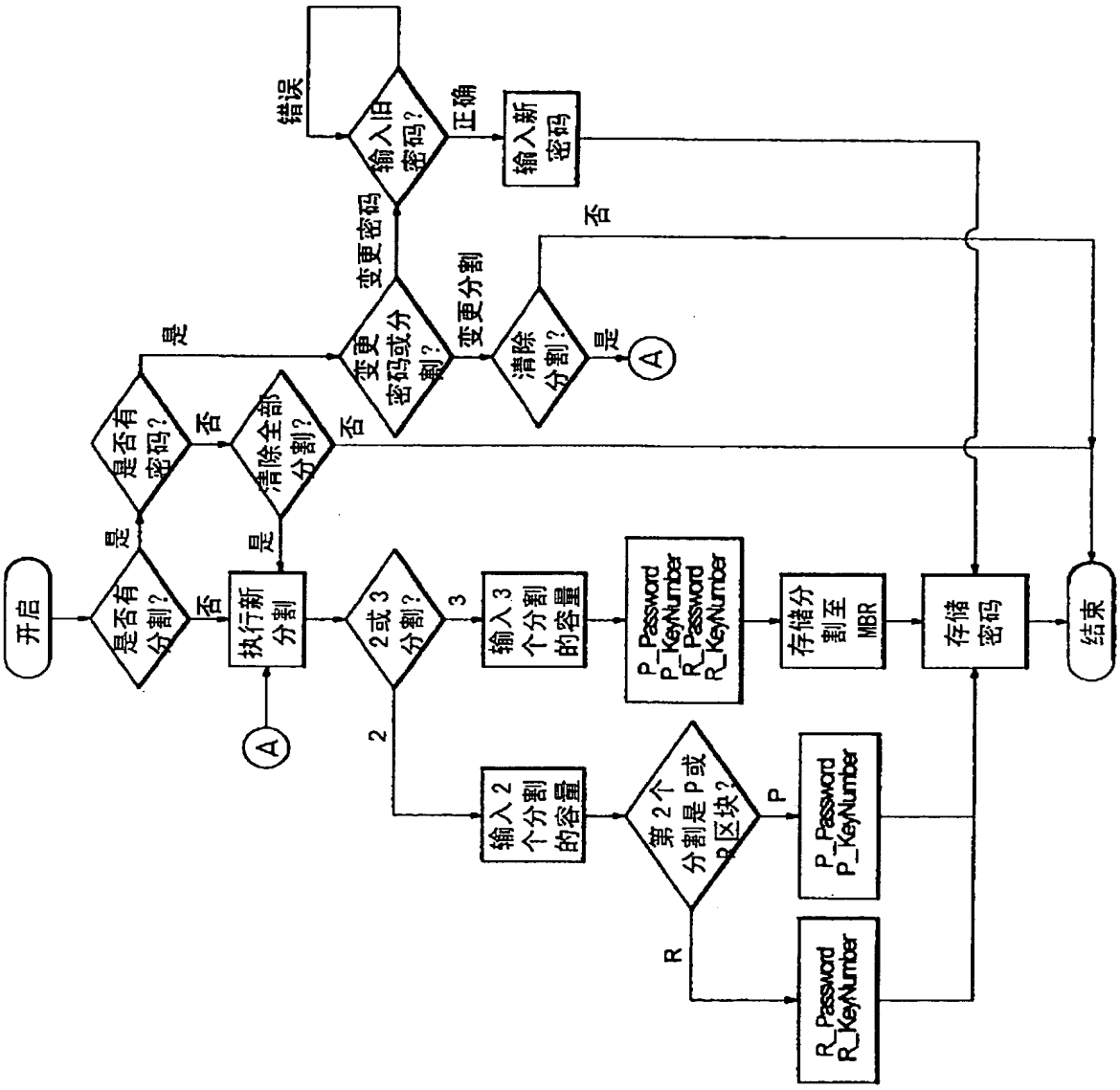

开启
是否有分割?
是
否
是否有密码?
是
否
清除全部分割?
是
否
执行新分割
A
2或3分割?
3
2
输入3个分割的容量
输入2个分割的容量
P_Password
P_KeyNumber
R_Password
R_KeyNumber
第2个分割是P或R区块?
P
R
P_Password
P_KeyNumber
R_Password
R_KeyNumber
存储分割至MBR
存储密码
结束
变更密码或分割?
是
否
变更密码
变更分割
清除分割?
是
否
A
输入旧密码?
错误
正确
输入新密码

图 1

Command	ROM zone	User zone	Protect zone
Check Power Mode - 98h or E5h	Executable	Executable	Executable
Execute Drive Diagnostic - 90h	Executable	Executable	Executable
Erase Sector(s) - C0h	Aborted	Executable	Aborted
Format Track - 50h	Aborted	Executable	Aborted
Identify Drive – Ech	Executable	Executable	Executable
Idle - 97h or E3h	Executable	Executable	Executable
Idle Immediate - 95h or E1h	Executable	Executable	Executable
Initialize Drive Parameters - 91h	Executable	Executable	Executable
Read Buffer - E4h	Executable	Executable	Executable
Read Multiple - C4h	Executable	Executable	Aborted
Read Long Sector - 22h or 23h	Executable	Executable	Aborted
Read Sector(s) - 20h or 21h	Executable	Executable	Aborted
Read Verify Sector(s) - 40h or 41h	Executable	Executable	Aborted
Recalibrate - 1Xh	Executable	Executable	Executable
Request Sense - 03h	Executable	Executable	Executable
Seek - 7Xh	Executable	Executable	Aborted
Set Features – Efh	Executable	Executable	Executable
Set Multiple Mode - C6h	Executable	Executable	Executable
Set Sleep Mode- 99h or E6h	Executable	Executable	Executable
Standby - 96h or E2h	Executable	Executable	Executable
Standby Immediate - 94h or E0h	Executable	Executable	Executable
Translate Sector - 87h	Executable	Executable	Aborted
Wear Level - F5h	Executable	Executable	Executable
Write Buffer - E8h	Executable	Executable	Executable
Write Long Sector - 32h or 33h	Aborted	Executable	Aborted
Write Multiple Command - C5h	Aborted	Executable	Aborted
Write Multiple without Erase – CDh	Aborted	Executable	Aborted
Write Sector(s) - 30h or 31h	Aborted	Executable	Aborted
Write Sector(s) without Erase - 38h	Aborted	Executable	Aborted
Write Verify - 3Ch	Aborted	Executable	Aborted
PQI Security Unlock - FEh	Executable	Executable	Executable

图 2

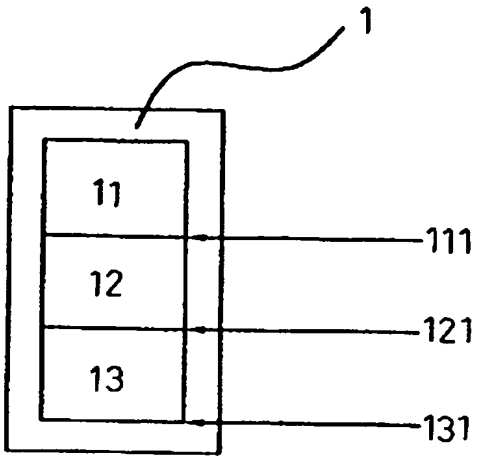

1
11
12
13
111
121
131

图 3

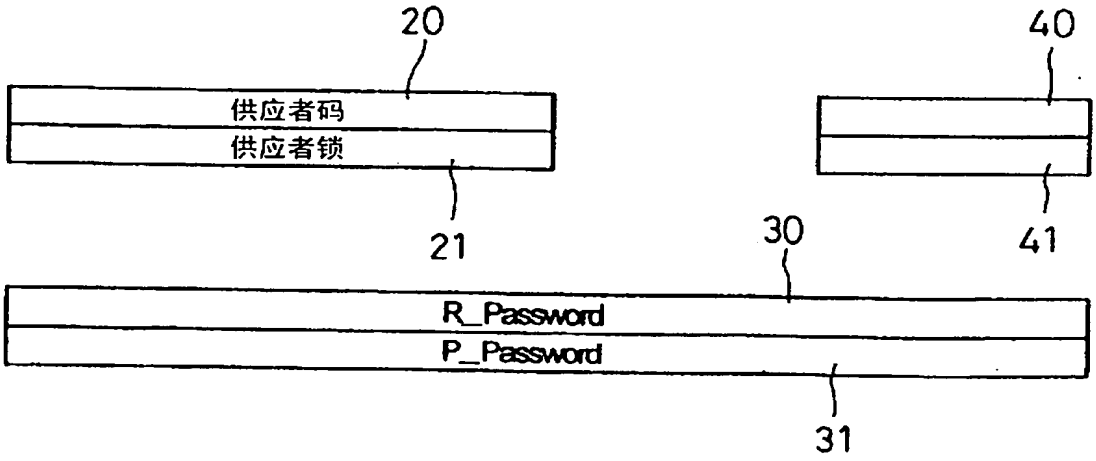

20
供应者码
供应者锁
21
40
41
30
R_Password
P_Password
31

图 4

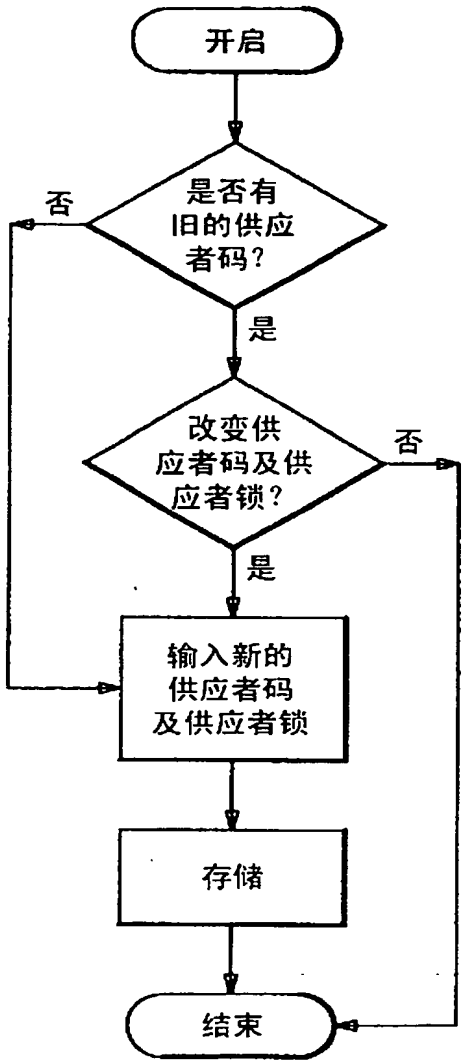


图 5

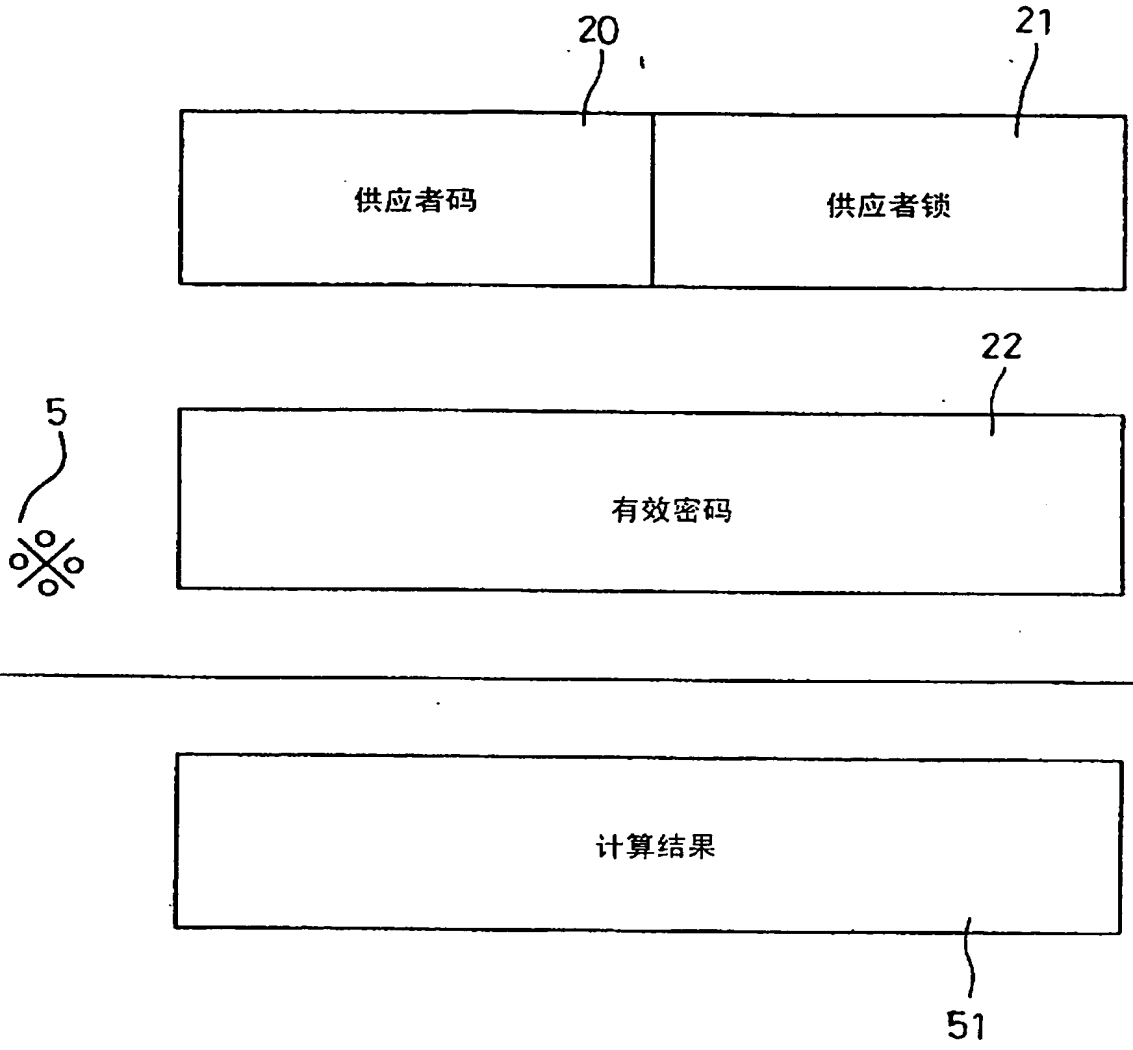


图 6

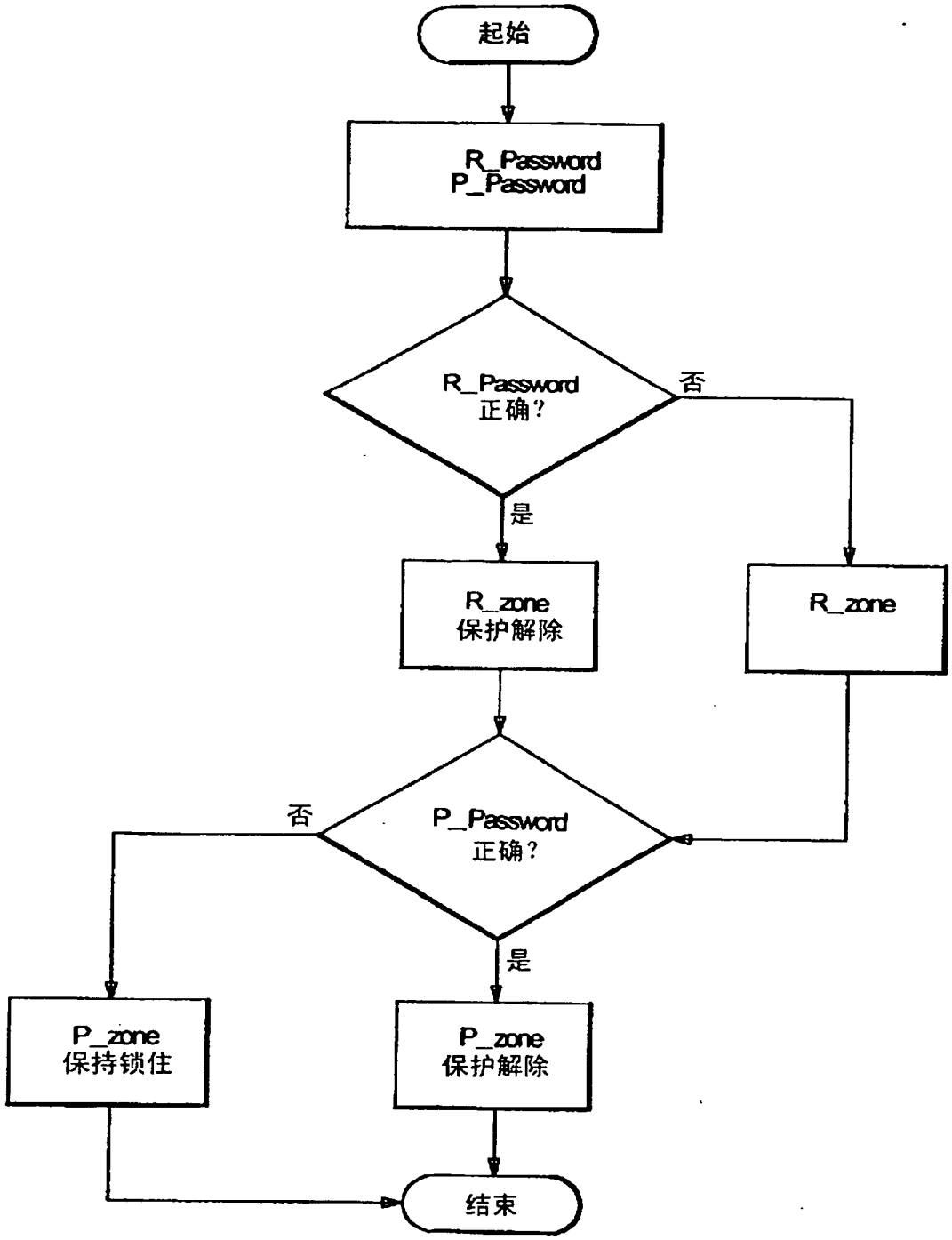

起始
R_Password
P_Password
R_Password
正确?
否
是
R_zone
保护解除
R_zone
P_Password
正确?
否
是
P_zone
保持锁住
P_zone
保护解除
结束

图 7